Journal of Combinatorial Theory, Series A **80**, 283–289 (1997)
Article No. TA972825

Ternary Covering Codes Derived from BCH Codes

John C. Cock

5 Wyddrington House, 55 Pittville Lawn, Cheltenham, Gloucestershire GL52 2BQ, England

and

Patric R. J. Östergård*

Department of Mathematics and Computing Science, Eindhoven University of Technology, P.O. Box 513, 5600 MB Eindhoven, The Netherlands

Communicated by the Managing Editors

It is shown how ternary BCH codes can be lengthened to get linear codes with covering radius 2. The family obtained has the ternary Golay code as its first code, contains codes with record-breaking parameters, and has a good asymptotic behavior. The ternary Golay code is further used to obtain short proofs for the best known upper bounds for the football pool problem for 11 and 12 matches. © 1997 Academic Press

1. INTRODUCTION

Let F_q^n denote the set of all n-tuples $(x_1, x_2, ..., x_n)$ over the finite field F_q of order q, where q is a prime power. The covering radius R of a code $C \subseteq F_q^n$ is the smallest integer such that every word in the space is within Hamming distance R from some word in C. If the code forms a linear subspace of F_q^n, it is said to be linear.

For given parameters, we want to find the minimum cardinality of a covering code. We here consider the case $q = 3$ and construct linear codes with $R = 2$ and nonlinear codes with $R = 1$. The minimum cardinality of a ternary code of length n and covering radius 1 is denoted by σ_n. The problem of determining σ_n is called the *football pool problem* as it gives the minimum number of forecasts in a football pool of n matches (with $q = 3$ alternatives for each match) such that at least one forecast has at least

* Present address: Department of Computer Science and Engineering, Helsinki University of Technology, P.O. Box 1100, 02015 HUT, Finland. E-mail: Patric.Ostergard@hut.fi. This author's research was supported by the Academy of Finland and the Walter Ahlström Foundation.

0097-3165/97 $25.00

$n-1$ (that is, $n-R$) correct results. For a recent survey of the football pool problem, see [9]. For a general survey of covering codes, the reader is referred to [2].

In Section 2 some properties of finite fields are discussed. In Section 3 linear codes with covering radius 2 are constructed by lengthening ternary BCH codes. The first code in the new series of linear codes is the ternary Golay code.

In Section 4 it is shown how this way of constructing the Golay code can be utilized to get new, short proofs of the following upper bounds for the football pool problem [8]: $\sigma_{11} \leqslant 9477$ and $\sigma_{12} \leqslant 27702$. The first bound is shown by a combinatorial proof in [8], while the second bound is proved in the same paper by giving a construction that can be checked by a computer. The codes obtained here are equivalent to the original codes in [8].

2. SOME PROPERTIES OF FINITE FIELDS

In what follows, α will be a generator of the field, and the abbreviations QR and QNR will mean respectively quadratic residue and quadratic non-residue. The proof of Lemma 1 is elementary and is omitted (see [7, Chap. 4, Theorem 13]).

LEMMA 1. *In F_q, if $q \equiv 1 \pmod 4$, then -1 is a QR (and the elements α^i and $-\alpha^i$ are either both QRs or both QNRs); if $q \equiv 3 \pmod 4$, then -1 is a QNR (and one of the elements α^i and $-\alpha^i$ is a QR and the other is a QNR).*

LEMMA 2. *In F_q, $q \geqslant 5$ odd, any nonzero element can be expressed as a sum of one QR and one QNR.*

Proof. If one nonzero element can be expressed as a sum, $x = \alpha^i + \alpha^j$ with i odd and j even, then every other nonzero element can be obtained as $\alpha^k x = \alpha^{i+k} + \alpha^{j+k}$ (one of $i+k$ and $j+k$ (modulo $q-1$) is even and the other is odd). For a given value of i, a required sum exists if there are at least two QRs, which is the case when $q \geqslant 5$. ▮

LEMMA 3. *In F_q, $q \geqslant 3$ odd, any QR can be expressed as a sum of two QNRs.*

Proof. We shall now show that there is at least one QR that can be expressed as a sum, $x = \alpha^i + \alpha^j$ with i, j odd. Then every other QR can be obtained as $\alpha^{2k} x = \alpha^{i+2k} + \alpha^{j+2k}$.

The lemma clearly holds for $q=3$, so we can assume that $q \geqslant 5$. Then Lemma 2 gives that any QNR can be obtained as a sum of a QNR and a QR. Take one such sum, $\alpha^{i'} = \alpha^i + \alpha^j$ with i, i' odd and j even. Now $\alpha^i + \alpha^0$, $\alpha^i + \alpha^1$,..., $\alpha^i + \alpha^{q-2}$ take all possible values of F_q, except $\alpha^i = \alpha^i + 0$, exactly once. As the $(q-1)/2$ values $\alpha^i + \alpha$, $\alpha^i + \alpha^3$, ..., $\alpha^i + \alpha^{q-2}$ contain neither α^i nor $\alpha^{i'}$, it follows that at least one of the values must be a QR. We have thus found a QR as a sum of two QNRs, as required. ▌

3. NEW TERNARY LINEAR COVERING CODES

In the construction to be presented, we lengthen ternary BCH codes. Let $l(r, R; q)$ denote the minimum length of a q-ary linear code of co-dimension r and covering radius R. We shall now state and prove the main theorem of this paper.

THEOREM 1. $l(4k+1, 2; 3) \leqslant (5 \cdot 9^k - 1)/4$.

Proof. To be able to utilize Lemma 1, we require that the order of the big field $3^{k'} \equiv 1 \pmod 4$, which is fulfilled exactly when k' is even: $k' = 2k$. Let $V = \{(1, \omega, \omega^2) \mid \omega \in F_{3^{2k}}\}$ (which are the column vectors of a parity check matrix for an extended ternary BCH code), and let $V' = \{(0, 0, v) \mid v \in F_{3^{2k}}$ takes one of the values of each pair x, $-x$ of QNRs$\}$ (cf. Lemma 1). Then each vector $(a, b, c) \in F_3 F_{3^{2k}} F_{3^{2k}}$ can be expressed in the following way as a linear combination over the small field (with coefficients modulo 3) of at most two vectors in $V \cup V'$:

$a = b = 0$:	Follows from Lemmas 1 and 3;
$a = 0$, $b \neq 0$:	$(1, u, u^2) - (1, v, v^2)$ with $v, u = -c/b \pm b$;
$a = 1$, $c - b^2 = 0$:	$(1, b, b^2)$;
$a = 1$, $c - b^2$ is a QR:	$-(1, u, u^2) - (1, v, v^2)$ with $u, v = b \pm \sqrt{c - b^2}$;
$a = 1$, $c - b^2$ is a QNR:	$(1, b, b^2) + (0, 0, c - b^2)$ or $(1, b, b^2)$ $-(0, 0, b^2 - c)$;
$a = 2$:	Follows from the solutions for $a = 1$ using $(2, b, c) = -(1, -b, -c)$.

The vectors in $V \cup V'$ can now be taken as column vectors of a parity check matrix for a ternary covering code with covering radius 2. The number of columns in the matrix is $((3^{2k} - 1)/4) + 3^{2k} = (5 \cdot 9^k - 1)/4$. ▌

The first code in the family of codes obtained, for $k = 1$, is the ternary Golay code. Ternary linear covering codes have recently been studied in

[3, 4]; Theorem 1 improves on several bounds in these papers. The new bounds lead to further improvements using

$$l(r+1, 2; 3) \leqslant 2l(r, 2; 3), \tag{1}$$

which is proven in [11] (and independently in [4]). The new bounds on $l(r, 2; 3)$ are given in Table I.

The asymptotic density of the new family of codes is better than for any other known families of ternary codes of covering radius 2. The *density* of a code C is defined by

$$\mu_q(n, R, C) = |C|\ V_q(n, R)/q^n,$$

where $V_q(n, R)$ is the number of words within Hamming distance R from a word in the space. For a perfect code, the density is clearly 1. For the codes produced by Theorem 1, the density tends to 25/24 as n tends to infinity.

If $r \equiv 3 \pmod 4$, we cannot use the full strength of Theorem 1, but we can still get the following bound, which gives one improvement in Table I.

THEOREM 2. $l(4k+3, 2; 3) \leqslant (9^{k+1}-1)/2$.

Proof. The proof goes exactly as the proof of Theorem 1 but now, as one of x and $-x$ is a QR and the other is a QNR if the order of the big field $3^{k'} \equiv 3 \pmod 4$ (see Lemma 1), we define the set V' to contain all QNRs. The total number of vectors in $V \cup V'$ then increases to $((3^{2k+1}-1)/2) + 3^{2k+1} = (9^{k+1}-1)/2$. ∎

TABLE I

New Upper Bounds on $l(r, 2; 3)$ for $r \leqslant 30$

r	[3, 4]	New Bound	Density	Construction
7	44	40	1.4636	Theorem 2
9	130	101	1.0366	Theorem 1
10	220	202	1.3821	(1)
13	971	911	1.0411	Theorem 1
14	1862	1822	1.3881	(1)
17	8734	8201	1.0416	Theorem 1
18	16753	16402	1.3888	(1)
21	78489	73811	1.0417	Theorem 1
22	150660	147622	1.3889	(1)
25	707494	664301	1.0417	Theorem 1
26	1357033	1328602	1.3889	(1)
29	6357609	5978711	1.0417	Theorem 1
30	12203460	11957422	1.3889	(1)

Other improvements for the case $r = 4k + 3$ (and further for $r = 4k$ using (1)) can probably be obtained if constructions similar to those in [3, 4] are applied to the codes from Theorem 1.

4. NEW PROOFS FOR THE FOOTBALL POOL PROBLEM

The construction presented in the previous section shall be used here to obtain good nonlinear covering codes. Short algebraic proofs of the best known upper bounds for the football pool problem for 11 and 12 matches will be given.

The following construction by Kamps and Van Lint [5] and Blokhuis and Lam [1] is used in the proofs in [8] and in the proofs to be presented here. (In the following, *cover* is used as a shorthand for *cover with covering radius* 1.) Let $M = \{m_1, m_2, ..., m_n\}$ be a set of words from F_q^r. We say that a set $S \subseteq F_q^r$ covers F_q^r using M if all words in F_q^r can be expressed in the form $s + \beta m_i$, where $s \in S$ and $\beta \in F_q$.

THEOREM 3 (Blokhuis and Lam, [1, Theorem 2.1]). *If S covers F_q^r using M, then $W = \{(w_1, w_2, ..., w_n) \in F_q^n \mid \sum_{i=1}^n w_i m_i \in S\}$ covers F_q^n. If M has rank r, then $|W| = |S|\, q^{n-r}$.*

We do not assume that M contains the r unit vectors. That form is assumed in [1], but—as pointed out in [6]—is not necessary.

We shall now use Theorem 3 to construct nonlinear ternary covering codes. A generalization of the following result is straightforward, but as the interest in the football pool problem concerns codes of short length ($n \leqslant 14$), we shall restrict ourselves to such codes. First we look at the football pool problem for 11 matches. For this code, we let

$$S = \begin{matrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 \\ \alpha & \alpha^3 & \alpha^5 & \alpha^7 & 0 & 1 & \alpha^2 & \alpha^4 & \alpha^6 & 1 & \alpha^2 & \alpha^4 & \alpha^6 \end{matrix}$$

and

$$M = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 \\ 1 & \alpha^2 & 0 & 1 & \alpha^2 & \alpha^4 & \alpha^6 & 1 & \alpha^2 & \alpha^4 & \alpha^6 \end{bmatrix}.$$

THEOREM 4. $\sigma_{11} \leqslant 9477 = 13 \cdot 3^6$.

Proof. Similarly to the proof of Theorem 1, we show that each vector $(a, b, c) \in F_3F_9F_9$ can be expressed as a sum of one vector in S (note that 0 is not in S) and a multiple of one vector in M:

$$\begin{aligned}
a=b=c=0: &\quad (1,0,0)-(1,0,0);\\
a=b=0,\ c\neq 0: &\quad \text{Follows from Lemmas 1 and 2;}\\
a=0,\ b\neq 0: &\quad (1,u,u^2)-(1,v,v^2) \text{ with } v,u=-c/b\pm b;\\
a=1: &\quad (1,b,b^2)+(0,0,c-b^2);\\
a=2,\ b^2+c \text{ is a QNR}: &\quad (0,0,b^2+c)-(1,-b,b^2);\\
a=2,\ b^2+c \text{ is a QR or 0}: &\quad (1,u,u^2)+(1,v,v^2) \text{ with}\\
&\quad u,v=-b\pm\sqrt{-b^2-c}.
\end{aligned}$$

The theorem now follows when Theorem 3 is applied. ∎

It is not difficult to see that another covering can be obtained by deleting the first two columns from M and adding the four columns $(0, 0, u)$, u a QR, to S. This covering gives the bound $\sigma_9 \leqslant 1377 = 17 \cdot 3^4$, which is also mentioned in [8] but is inferior to the presently best known bound, $\sigma_9 \leqslant 1341 = 149 \cdot 3^2$, proved in [10].

Now we proceed with the case $n = 12$. The proof of the following lemma is a matter of direct calculations. (We use the notations $\lambda S = \{\lambda s \mid s \in S\}$ and $S + s' = \{s + s' \mid s \in S\}$.)

LEMMA 4. *If S covers F_q^r using M, then $S + s$ covers F_q^r using M for any $s \in F_q^r$.*

Let c be any of the first four columns of S, say $c = (0, 0, \alpha)$, and let S and M be as above. We define the following sets S' and M' in $F_3F_9F_9F_3$: $S' = (S + c) \oplus \{1\} \cup (2S + c) \oplus \{2\} \cup (S \setminus \{c\}) \oplus \{0\}$ (so $|S'| = 38$) and $M' = M \oplus \{0\} \cup \{(0, 0, 0, 1)\}$.

THEOREM 5. $\sigma_{12} \leqslant 27702 = 38 \cdot 3^6$.

Proof. We shall show that every vector in $F_3F_9F_9F_3$ can be expressed as a sum of one vector in S' and a multiple of one vector in M'. The vectors $(S + c) \oplus \{1\}$ and $(2S + c) \oplus \{2\}$ cover all vectors with a 1 and 2, respectively, in the last coordinate using $M \oplus \{0\}$. This follows from Theorem 4, Lemma 4, and the fact that $2S$ can be substituted for S in the construction for Theorem 4. The vectors $(S \setminus \{c\}) \oplus \{0\}$ cover all vectors with a 0 in the last coordinate using $M \oplus \{0\}$, except possibly for the vectors $\{c\} \oplus \{0\}$, $(M + c) \oplus \{0\}$, and $(2M + c) \oplus \{0\}$. However, all vectors $(0, 0, x, 0)$ except the all-zero vector can still be obtained as it turns out that every $x \neq 0$ in F_9 is expressible as a sum of a QR and a QNR

without using α. Finally, the rest of the vectors can be expressed as a sum of a vector in $(S+c)\oplus\{1\}$ or $(2S+c)\oplus\{2\}$ and a multiple of $(0, 0, 0, 1) \in M'$. The theorem follows when Theorem 3 is applied. ∎

ACKNOWLEDGMENTS

The authors gratefully acknowledge the helpful comments from Alexander Davydov and the referees.

REFERENCES

1. A. Blokhuis and C. W. H. Lam, More coverings by rook domains, *J. Combin. Theory Ser. A* **36** (1984), 240–244.
2. G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, "Covering Codes," North-Holland, Amsterdam, 1997.
3. A. A. Davydov, Constructions and families of covering codes and saturated sets of points in projective geometry, *IEEE Trans. Inform. Theory* **41** (1995), 2071–2080.
4. A. A. Davydov, On nonbinary linear codes with covering radius two, *in* "Proceedings of the Fifth International Workshop on Algebraic and Combinatorial Coding Theory," pp. 105–110, Unicorn, Shumen, Bulgaria, 1996.
5. H. J. L. Kamps and J. H. van Lint, A covering problem, *Colloq. Math. Soc. János Bolyai* **4** (1970), 679–685.
6. P. J. M. van Laarhoven, E. H. L. Aarts, J. H. van Lint, and L. T. Wille, New upper bounds for the football pool problem for 6, 7, and 8 matches, *J. Combin. Theory Ser. A* **52** (1989), 304–312.
7. F. J. MacWilliams and N. J. A. Sloane, "The Theory of Error-Correcting Codes," North-Holland, Amsterdam, 1977.
8. P. R. J. Östergård, New upper bounds for the football pool problem for 11 and 12 matches, *J. Combin. Theory Ser. A* **67** (1994), 161–168.
9. P. R. J. Östergård, The football pool problem, *Congr. Numer.* **114** (1996), 33–43.
10. P. R. J. Östergård, Constructing covering codes by tabu search, *J. Combin. Des.* **5** (1997), 71–80.
11. P. R. J. Östergård, New constructions for q-ary covering codes, *Ars Combin.*, to appear.